Guidance, Navigation & Control (GN&C) Best Practices for Human-Rated Spacecraft Systems

Neil Dennehy
NESC

Dr. Ken Lebsock
Orbital Sciences

John West
Draper Laboratory

Program Management Challenge 2008
Daytona Beach, FL
26-27 February 2008

Presentation Outline

- **Introduction and Acknowledgements**
- **Motivation for the NESC GN&C Best Practices**
  - Common GN&C Pitfalls
- **Some Key GN&C System Considerations for Human-Rated Spacecraft**
  - GN&C related anomalies on crewed spacecraft
- **NESC's 22 GN&C Best Practices**
  - 15 for "Early Work" and 7 for "Late Work"
- **Discussion of Best Practices vs. Real-World Mishaps**
  - Review of the Progress M-34, LEWIS, X-31A, and Ariane-5 mishaps
- **Recommendations & Summary**

Introduction & Acknowledgements

Introduction

- **In 2007 the NESC completed an in-depth assessment to identify, define and document engineering considerations for the Design Development Test and Evaluation (DDT&E) of human-rated spacecraft systems**
  - Requested by the Astronaut Office at JSC to help them to better understand what is required to ensure safe, robust, and reliable human-rated spacecraft systems
- **The 22 GN&C engineering Best Practices described in this paper are a condensed version of what appears in the NESC Technical Report**
- **These Best Practices cover a broad range from fundamental system architectural considerations to more specific aspects (e.g., stability margin recommendations) of GN&C system design and development**
- **15 of the Best Practices address the early phases of a GN&C System development project and the remaining 7 deal with the later phases.**
  - Some of these Best Practices will cross-over between both phases.
- **Recognize that this initial set of GN&C Best Practices will not be universally applicable to all projects and mission applications**

Acknowledgements

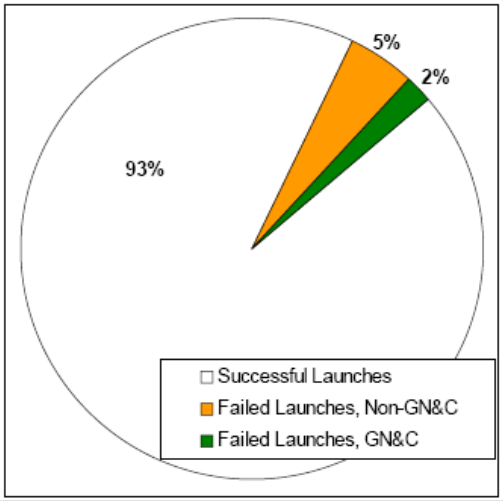
The GN&C section of the NESC DDT&E "Engineering Considerations" Report, upon which this presentation is based, was the product of the work and inputs of several individuals in addition to the authors, including but not limited to:

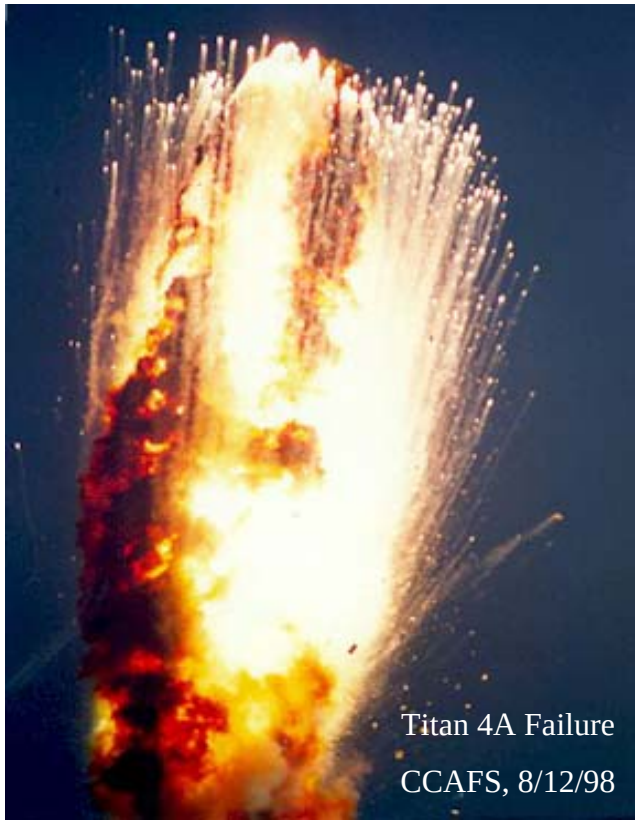
- **Jim Blue, Scott Miller (Orbital)**
- **Mike Cleary, Jerry Gilmore, Phil Hattis, Dorothy Poppe (Draper Laboratory)**
- **Bruce Jackson along with other members of the NESC GN&C TDT**
- **James Miller and Christina Cooper (NESC/LaRC)**
- **Ahmed Omar Amrani, Nichols F. Brown (Aerospace Corporation)**

Motivation for the NESC GN&C Best Practices

GN&C Related Worldwide Launch Vehicle Failures

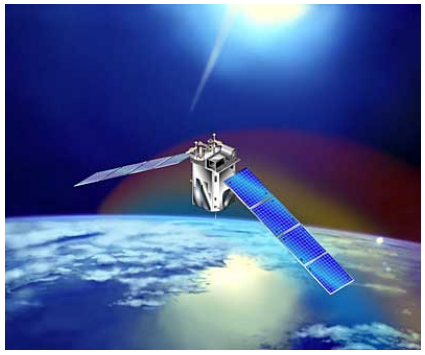
- **Over the ten year period of 1996 to 2006, 21 out of the 773 launch attempts worldwide, experienced a known GN&C anomaly**
  - 15 resulted in a catastrophic launch failure
- **Approximately one-third (15) of all 52 catastrophic launch failures worldwide over this ten year period were GN&C-related**
- **Design flaws identified as largest (40%) single cause of GN&C-related catastrophic launch failures (6 out of 15)**
- **Avionics and Flight Software were equally large (20%) failure causes at the component level**

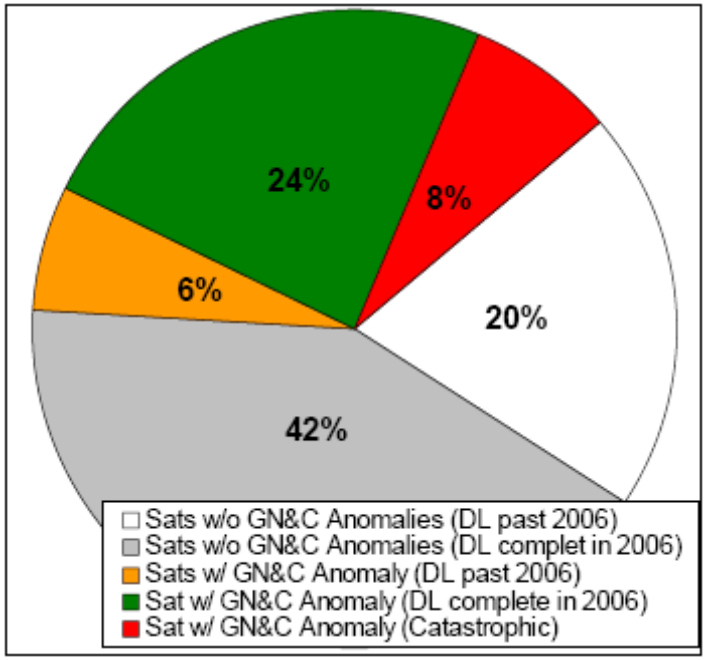



Titan 4A Failure
CCAFS, 8/12/98

GN&C Related NASA Spacecraft Failures

- Over the ten year period of 1996 to 2006, 38% (30 out of 79) of all NASA robotic spacecraft experienced a GN&C anomaly
- 8% of all NASA robotic spacecraft experienced a catastrophic failure over this same time period
- 50% of catastrophic GN&C anomalies occurred within 10% of the spacecraft's design life
- Largest contributing causes of catastrophic GN&C anomalies were:
  - Design (33%)
  - Software (33%)
  - Operational (17%)





Motivation for The NESC Best Practices

- **The primary motivation of this presentation is to provide useful guidance, in the form of these Best Practices, to the synthesis and operation of GN&C systems for NASA's future human-rated spacecraft.**

- **The GN&C Best Practice information contained in NESC Technical Report is also intended to provide:**
  - Insights for non-GN&C engineers and managers
  - Tutorial-type guidance for fresh-out GN&C engineers
  - A useful memory aid for more experienced GN&C engineers, especially as a checklist for technical evaluation and review of a GN&C system.

- **A secondary motivation of this presentation is to obtain feedback on this initial set of Best Practices from the NASA Program Management community**
  - In particular, we solicit other specific GN&C Lessons Learned that NESC should capture based on either crewed and robotic flight system project experiences

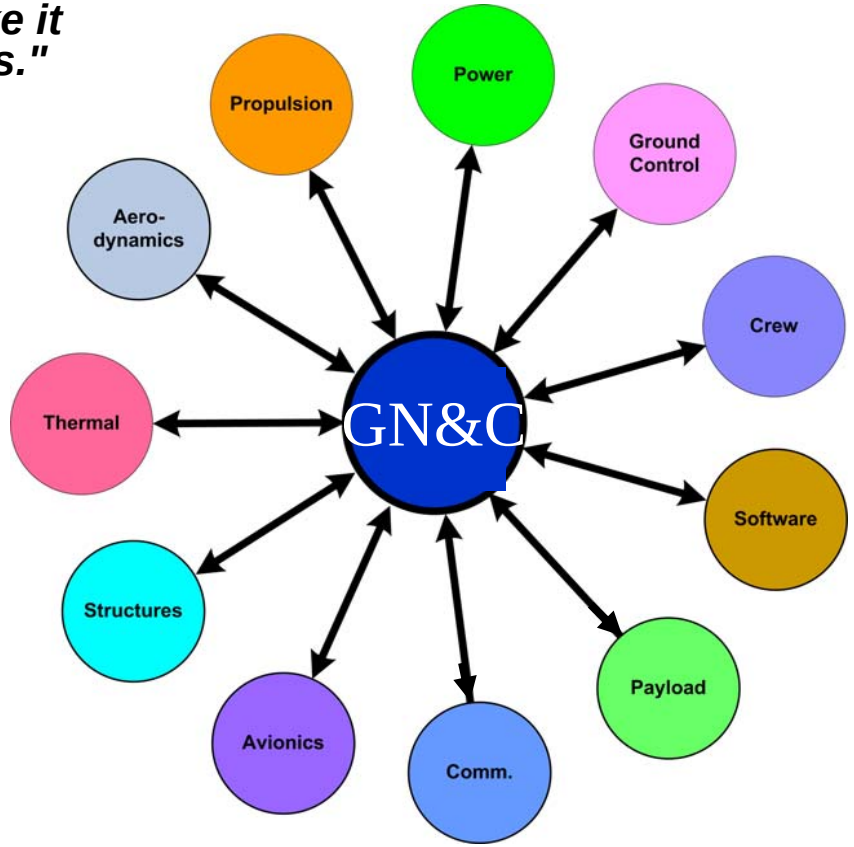
GN&C Interacts With, and is Influenced by, Virtually All Other Spacecraft Subsystems

"...we cannot do just one thing. Whether we like it or not, whatever we do has multiple effects."

Dietrich Domer, author of the Logic of Failure, commenting on the topic of complex systems

"In space systems, most dynamic problems do not occur in one isolated discipline, but are an interaction between several disciplines or subsystems"

Bob Ryan, author of "Problems Experienced and Envisioned for Dynamical Physical Systems[1]", commenting on his Apollo, Skylab, and Space Shuttle career experiences at NASA



GN&C engineers must consistently think at the system-level

[1] NASA Document TP-2508, August 1985

Common GN&C DDT&E Pitfalls (1 of 2)

- ✓ Poor or Missing GN&C Requirements
- ✓ Failure to Stop Requirements Creep
- ✓ Poor Characterization of Mission Operational Regimes & Environments
- ✓ Unknown or Poorly Defined Interactions
- ✓ Unknown or Poorly Defined Interfaces
- ✓ Poorly Defined Coordinate Frames and System of Units
- ✓ Unknown and/or Incorrectly Modeled Dynamics
- ✓ Feedback Control System Instabilities due to Large Model Uncertainties
- ✓ Reliance on Any “Heritage”: in the Hardware, Software, Design Team, etc.
- ✓ Reliance on low Technology Readiness Level (TRL) GN&C technologies
- ✓ Sensor/Actuator Component Degradation & Failure
- ✓ Insufficient On-Board Processing Capability for GN&C Flight Software (FSW) Algorithms

Common GN&C DDT&E Pitfalls (2 of 2)

- ✓ Inadequate Systems Engineering for Coordinated GN&C of Multiple Interacting Vehicles (e.g., during Rendezvous and Docking)
- ✓ Poor GN&C Fault Management Strategy
- ✓ Lack of Comprehensive Abort Strategy
- ✓ Inadequate “Safe Haven” capabilities
- ✓ Failure to “Design for Test”
- ✓ Failure to “Test as You Fly and Fly as You Test"
- ✓ Inadequate Hardware In The Loop (HITL) End-to-End Testing to Verify Proper Operations
- ✓ Inadequate Sensor-to-Actuator Polarity Tests (Lack of End-to-End Testing)
- ✓ Unresolved Test Anomalies & Discrepancies
- ✓ No truly independent Verification and Validation (V & V) process for GN&C
- ✓ Failure to Have Crew and Operations Team “Train as You Fly"
- ✓ Inadequate Validation/Certification of GN&C Ground Data and Tools
- ✓ Insufficient Telemetry for GN&C Performance Monitoring and Anomaly Resolution During Launch, Early Orbit Checkout & All Mission Critical Events

Motivation for The NESC Best Practices

- An examination of the historical record reveals that several NASA spacecraft GN&C systems have been seriously victimized by one of more of the pitfalls listed above either during their design, development, test or operational phases.
- It appears that many previously established Lessons Learned must be relearned by the community of practice as the institutional memory fades
- The continued repetition of the same GN&C mistakes represents an avoidable risk to crew safety and mission success.
- If rigorously followed these GN&C Best Practices will help protect against the pitfalls cited above.
- Bear in mind however that these GN&C Best Practices will not be universally applicable to all projects and mission applications.
- These GN&C Best Practices alone are not a substitute for sound engineering judgment, experience, expertise, attention to day-to-day details, and, most importantly, intellectual curiosity.

Motivation for The NESC Best Practices

Two Representative Examples Where Breakdowns in the Application of the GN&C Best Practices Occurred

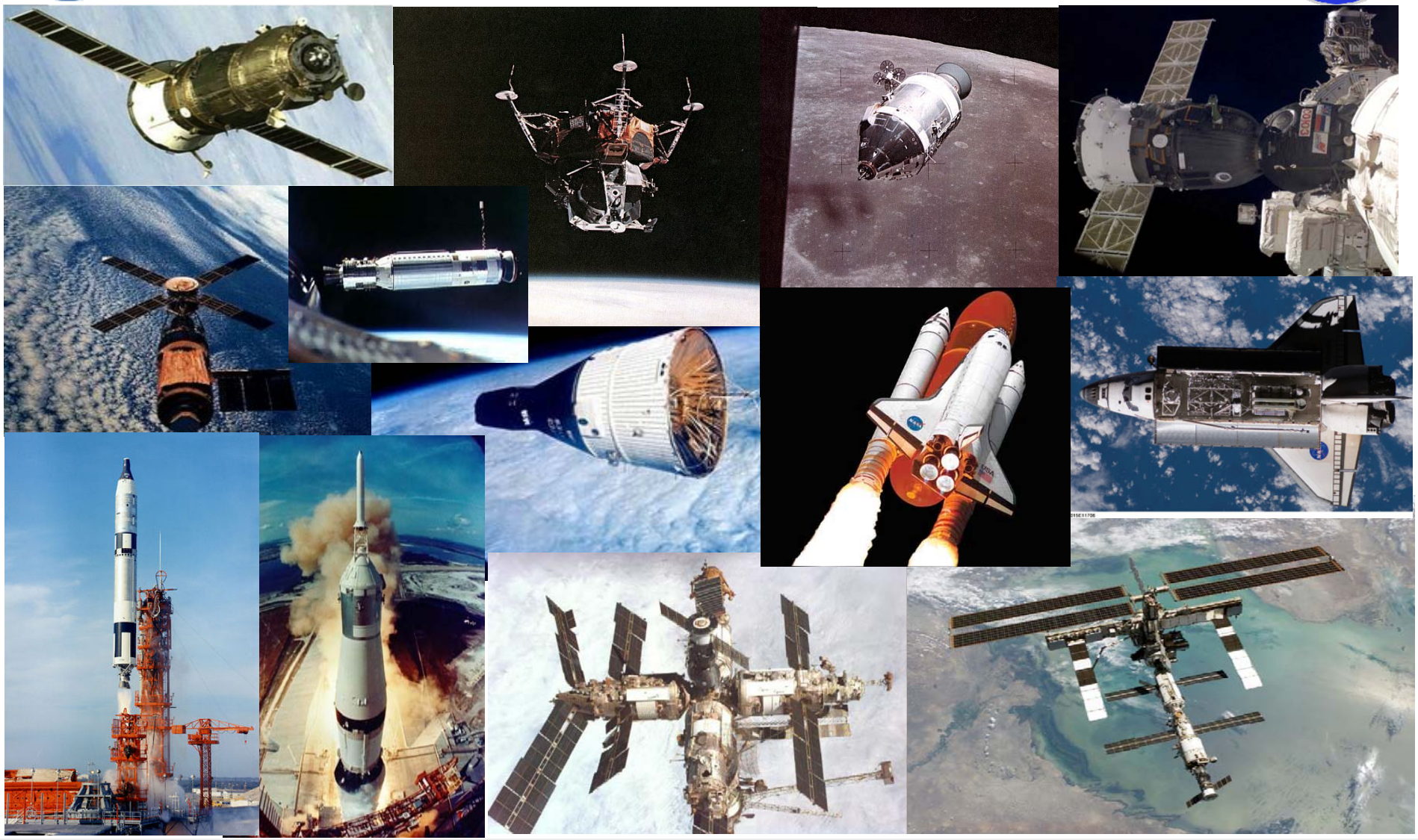
NASA Dryden Flight Research Center Photo Collection
http://www.dfrc.nasa.gov/gallery/photo/index.html
NASA Photo: EC01-0182-11 Date: June 2, 2001 Photo by: Jim Ross
The X-43A/Pegasus combination dropped into the Pacific Ocean after losing control early in the first free-flight attempt.

X-43A / Pegasus Launch June 2, 2001

Ariane 5 Flight 501 June 4, 1996

Some Key GN&C System Considerations for Human-Rated Spacecraft

Human Spaceflight Heritage:
A Significant GN&C Legacy to Study & Learn From



Significant GN&C Related Anomalies on Crewed Spacecraft

Gemini 8 March 1966

Failed "On" thruster causes vehicle to tumble; crew uses re-entry thrusters to recover attitude

Skylab Nov 1973

Control Moment Gyro (CMG) failure

Progress M-7 March 1991

Aborted Progress docking leads to near-miss encounter with Mir space station due to Kurs radar damage

Apollo 13 April 1970

O_2 tank explosion and EPS loss forces crew into LM "Lifeboat"; necessitates manual IMU alignment transfer from LM to CM platform prior to re-entry

Apollo 10 May 1969

LM tumbles while in low lunar orbit; IMU gimbal lock narrowly avoided during attitude recovery by crew

STS-51F July 1985

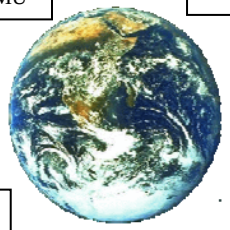
Abort to Orbit performed following a premature SSME shutdown during ascent due to false engine overheating indications

STS-9 Nov 1983

Landing delayed due to 2 GPC failures and an IMU

STS-91 June 1991

Primary Avionics Software System (PASS) corrupted by GPS errors



ISS June 2007

Loss of thruster based attitude control due to Russian computer outage

Soyuz TM-17 Jan 1994

Collides twice with Mir

Apollo 11 July 1969

LM guidance computer overloads during powered descent

Soyuz 18-1 April 1975

First high altitude abort of a crewed spacecraft when 2nd stage fails to separate from 3rd stage of booster; crew survives 20 g reentry

Progress M-34 June 1997

Collides with Mir

Apollo 14 Feb 1971

Faulty LM abort mode switch delays landing six hours

ISS June 2002

Control Moment Gyro (CMG) failure

STS-3 March 1982

Dynamic interaction between Orbiter flight control system and robotic arm motion causes unexpectedly high vernier thruster duty cycles

STS-1 April 1981

Unmodeled vernier thruster plume impingement causes greatly increased duty cycles and propellant consumption

Apollo 12 Nov 1969

Saturn-V booster struck by lighting; IMU in Command Module tumbles & crew looses attitude reference

Soyuz T-10A Sept 1983

First pad abort of a crewed spacecraft after pad fire; crew survives 17 g Launch Escape System flight

STS-1 April 1981

Significant unpredicted Orbiter rocking motion on ET, when SSME's slewed to stow position, causes cyclic pitch thruster firings

Soyuz Ballistic Re-Entries

Soyuz 33 April 1979 10 g's

Soyuz TMA-1 May 2003 8 g's

Soyuz TMA-10 Oct 2007 9 g's

STS-3 March 1982

Handling Qualities (PIO) problem occurs; causes unintended Orbiter pitch-up during landing rollout

Some General Observations on Significant Human Space Flight GN&C Anomalies

- **Several significant GN&C related anomalies have occurred: fortunately, none resulting in the loss of human life**
- **Anomalies have occurred during ascent, on-orbit, Entry, Descent and Landing (EDL) mission phases**
  - Anomalies have occurred during Earth, Mars and Lunar landings
- **In most anomaly cases, other than the highly dynamic ascent and reentry mission phases, the crew (and the ground) had time to evaluate, troubleshoot, and respond to GN&C anomalies**
- **Many of the GN&C subsystems had superior architectural attributes that anticipated, accommodated and supported the recovery from failures, degraded modes of operation, and anomalistic behaviors**
- **It several cases it appears the spacecraft GN&C robustness precluded a significant anomaly from becoming catastrophic**

Some Key GN&C System Considerations for Human-Rated Spacecraft (1 of 2)

- **Take time to properly architect the GN&C subsystem**
  - OS&MA analysis identified that 70-90% of the safety-related decisions in NASA's engineering projects are made during early concept development.
  - Directly impacts crew safety, mission success, upgradeability & system Life Cycle Costs
  - Carefully trade identical vs. diverse GN&C hardware components and software elements when considering redundancy

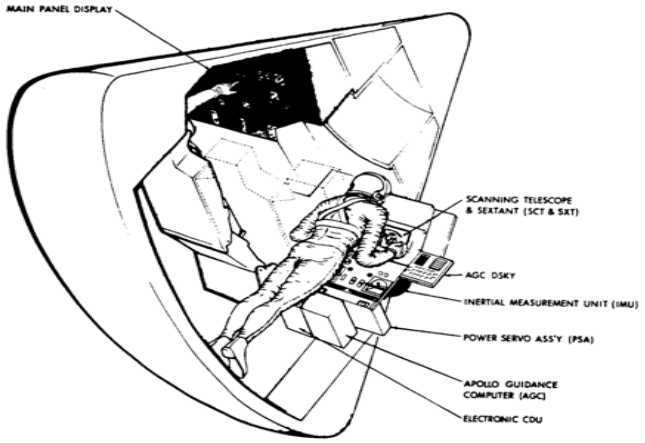
- **Minimize complexity where possible**
  - Impacts reliability, testability, and operability, as well as potential for GN&C subsystem commonality across multiple space systems

- **Formulate robust abort strategies and implement reliable Safe-Haven capabilities**
  - These are an integral part of a sound layered defense/safety net
  - Absolutely need a simple "Never Give Up" Safe-Haven backup mode capable of returning the crew safely to Earth

Some Key GN&C System Considerations for Human-Rated Spacecraft (2 of 2)

- **Carefully evaluate the cost/benefit trade for all heritage hardware and software when doing the Design-Rebuild-Procure trade**
  - Be skeptical of the "shelf"
  - Recall Shuttle issues with tactical aircraft heritage:
    - Inertial systems,
    - GPS receivers,
    - and processors

Apollo Hybrid Simulator



- **"Train as You Fly" Approach Can Influence GN&C**
  - Seek early crew feedback on GN&C architecture, human-machine interface, and nominal/contingency operational procedures
  - Flight-like cockpit mockups (such as the Apollo Hybrid Simulator) allowed Apollo astronauts early hands-on training which influenced that GN&C design

Shuttle Avionics Integration Lab

NESC's 22 GN&C Best Practices:

15 for "Early Work" and 7 for "Late Work"

List of the NESC 15 Early Work GN&C Best Practices

1. Early and iterative GN&C subsystem architectural development
2. Define all GN&C interdisciplinary interactions and relationships
3. Ensure implementation of comprehensive Abort/Safe Haven strategies/functions
4. Adequacy of host computer and proper selection of execution frequencies
5. Independent hardware and software for GN&C fault management
6. Establish & flowdown GN&C requirements for multi-vehicle system
7. Evaluate redundancy with identical GN&C hardware components
8. Evaluate heritage hardware and software in the GN&C architecture
9. Make certain that new GN&C technology is well qualified
10. "Design for Test" when evaluating candidate GN&C architectures
11. Define and document the coordinate frames and the system of units
12. Controller designs shall have robust stability margins
13. Understand & completely analyze the dynamics in ALL flight phases
14. All test anomalies must be understood and may need to be included in the truth model
15. Verification Truth Model must be developed independently

List of the NESC 7 Late Work GN&C Best Practices

16 Establish a strong relationship with, and maintain close surveillance of GN&C lower-tier component-level suppliers

17 Adhere to the “Test As You Fly” philosophy

18 Conduct true end-to-end sensors-to-actuators polarity tests in all flight configurations

19 Plan and conduct sufficient GN&C hardware-in-the-loop testing to verify proper interactions

20 Carefully manage GN&C ground databases, uploads, ground application tools, and command scripts / files

21 Ensure sufficiency of GN&C engineering telemetry data

22 “Train as They Fly”: Develop a dedicated real-time GN&C simulator for the crew/operators

NESC GN&C DDT&E Best Practices References

1) A convenient single page formated description of each of the 22 NESC GN&C DDT&E Best Practices listed above is given in the paper AIAA-2007-6336, *"GN&C Engineering Best Practices for Hunan-Rated Spacecraft Systems",* dated August 2007, by Dennehy/Lebsock/West

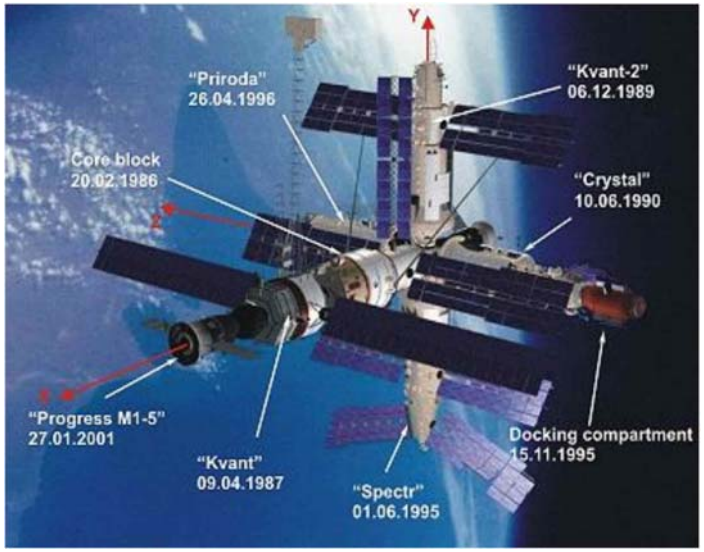
2) A much more detailed description and discussion of each of the Best Practices is given in Section 7 of the NASA Engineering and Safety Center Technical Report, NESC Document # RP-06-108, *"Design, Development, Test, and Evaluation (DDT&E) Considerations for Safe and Reliable Human Rated Spacecraft Systems Volume II"* which can be downloaded from:

www.nasa.gov/pdf/189071main_RP-06-108_05-173_DDT&_E_Volume_II_(MASTER)08-07-2007_Final_%5B1%5D.pdf

Discussion of Best Practices
vs.
Real-World Mishaps

Top-Level Summary of the Progress M-34 Mishap

- **Progress-M spacecraft are unmanned cargo and resupply vehicles used to send equipment to Mir.**
- **On 6/25/97 a 2nd test was performed of the manual Toru proximity docking system as a lower cost substitute for the autonomous Kurs rendezvous and docking system.**
- **Operator on Mir had difficulty determining range and range rate with the Kurs radar switched off.**
- **Progress M-34 went off course and collided with a solar array and radiator on the Spektr module and then the module itself.**
- **Spektr hull was breached causing significant air loss before Spektr module could be sealed off.**
- **Evacuation of the station was narrowly avoided.**
- **There were three immediate causes of the crash:**
  - The higher than planned initial closing rate
  - Late realization that closing rate was too high
  - Incorrect final avoidance maneuvering



Root Causes of the Progress M-34 Mishap vs. NESC GN&C Best Practices

1. **Range was to be determined by observing the size of a video image of Mir taken by a camera on Progress. The sole source of range rate information was the changing angular size and position of the image.**

   BP #9: *The range rate measurement scheme was not qualified.*

   BP #5: *No independent way was provided to determine a fault in the range rate measurement.*

2. **The operator continued to maneuver and aim for the docking port after noticing that the closing rate was higher than expected.**
   BP #14: *Failure to explain test anomalies.*

3. **Post crash simulations show that the rendezvous trajectory was passively safe so that if the operator had stopped maneuvering in time the collision might have been avoided.**

   BP #6: *Pre-test Systems Engineering did not flow down appropriate requirements to insure the safe interaction between the vehicles.*

   BP #3: *Opportunity for passive abort option not taken advantage of.*

4. **The operator could not realistically train and rehearse the rendezvous in advance because there were no simulation training facilities onboard Mir.**
   BP #22: *There was no provision to "Train as They Fly".*

Top-Level Summary of the LEWIS Mishap

LEWIS was launched on August 23, 1997 into low Earth Orbit.

The LEWIS GN&C subsystem design drew heavily from the TOMS-EP spacecraft heritage.

1. **At launch, LEWIS was under control of the A-side processor. At first contact it had already switched to the B-side and was unable to playback SSR data.**
2. **After 45 hours of nadir pointing on B-side, the Ground crew switched control back to the A-side. The attitude was uncontrolled so the A-side Sun pointing mode was entered.**
3. **After verifying that the spacecraft had been stable in the Sun mode for four hours of operation, the Ground crew entered a nine-hour rest period and ceased operations for the day.**
4. **During that unattended period, the spacecraft entered a flat spin that resulted in a loss of solar power and a fatal battery discharge. Contact with the spacecraft was lost on August 26.**
5. **The spacecraft re-entered the atmosphere and was destroyed on September 28, 1997.**

Root Causes of the LEWIS Mishap vs. NESC GN&C Best Practices

1. **Safe mode was adapted from the TOMS spacecraft which had its X-axis normal to the solar array. The X-axis was the major moment-of-inertia axis on the TOMS-EP spacecraft but it was the intermediate moment-of-inertia axis on Lewis.**
   - **BP #8: *Over-reliance/Over-Confidence on TOMS heritage.***
   - **BP #1: *GN&C Safe mode architectural was not iterated.***
2. **X-axis spin rate was not sensed and could not be controlled.**
   - **BP #3: *Ensure implementation of comprehensive Abort/Safe Haven strategies/functions.***
3. **The Ground crew failed to adequately monitor spacecraft health and safety during the critical initial mission phase.**
   - **BP #21: *Ensure sufficiency of GN&C engineering telemetry data.***
4. **X-axis rate produced disturbance torques in other axes resulting in excessive thruster firings which led to autonomous shutdown of thrusters.**
   - **BP #13: *Understand & completely analyze the dynamics in ALL flight phases.***
5. **In the absence of control, the spacecraft dynamics transferred spin from the X to the Z axis with the solar array edge on to the Sun.**
   - **BP #15: *Independent Truth Model should have identified un-modeled effects.***

Top-Level Summary of the X-31A Mishap

The X-31 program demonstrated the value of Thrust Vector Control (TVC) coupled with advanced flight control systems, to provide controlled flight during close-in air combat at very high angles of attack.

- **The final flight of the X-31A was through atmospheric conditions conducive to icing.**
- **The flight went as planned until an ice buildup blocked the pitot tube.**
- **The Flight Computer used invalid air speed data to generate attitude control commands.**
- **Inappropriate commands resulted in uncontrollable/divergent pitch oscillations.**
- **The pilot ejected at 18,000 ft. and parachuted to the ground.**
- **A NASA mishap-investigation board concluded that an accumulation of ice in or on the unheated pitot-static system was the proximate cause of the crash.**
- **Underlying Issues included:**
  - –Incomplete/improper interpretation of hazards analysis
  - –Breakdown in configuration management and change documentation
  - –Failure to impose proper ops controls and take preventative action

Root Causes of the X-31A Mishap vs. NESC GN&C Best Practices

1. **The decision to install a new airspeed probe without a heater assumed that no flights would be made through conditions conducive to icing. The test pilot was unaware that the pitot heater switch was not working.**
   - **BP #10: *Failure to design for test.***
   - **BP #20: *Failure to coordinate information on potential hazard due to change in configuration.***
2. **Spurious air speed readings were noticed as ice built up and pilot switched ON the inoperative heater. Control room debated and finally replied that heater "…may not be hooked up" 9 seconds before warning tone and master caution light came on.**
   - **BP #14: *Failure to explain test anomalies.***
3. **When the Flight control computers received erroneous airspeed inputs, flight control gains changed so drastically that the pilot could not maintain control.**
   - **BP #12: *Insufficient control system stability margins.***
   - **BP #13: *Lack of parametric uncertainty analysis for control system.***
4. **'Fall-back' fixed gain reversion modes were available for such situations, but had not been practiced and the pilot had not been briefed on their potential use in the event of unreliable airspeed data.**
   - **BP #3: *Abort/Safe Haven strategy (Reversion Mode) was not utilized.***
5. **Data from alternate air speed indicator that used a different pitot tube was ignored.**
   - **BP #7: *Independent air speed sensor data was available but not utilized.***

Top-Level Summary of the ARIANE-5 Flight 501 Mishap

The maiden flight of the Ariane 5 launcher on June 4, 1996 relied on identical GN&C hardware and software for redundancy.

- **39 seconds into the flight the primary Inertial Reference Unit (SRI-1) stopped sending correct attitude data due to a software exception.**
- **The On-Board Computer (OBC) switched to the backup inertial unit, but SRI-2 also failed due to its independently determined (and identical) software exception.**
- **The OBC could not switch back to SRI-1 so it took data that was actually part of a diagnostic message written to the bus by SRI-2. This data was interpreted as flight data and used for Thrust Vector Control (TVC).**
- **The sudden swivelling of both solid booster nozzles up to the limit caused the launcher to tilt sharply giving rise to intense aerodynamic loads leading to destruction of the vehicle.**

Root Causes of the ARIANE-5 Flight 501 Mishap vs. NESC GN&C Best Practices

1. **Primary Inertial Reference Unit, SRI-1, stopped sending correct attitude data due to a software exception.**

   BP #2: *Interactions between S/W and GN&C were not defined with enough care.*
   BP #8: *Heritage software for Ariane-4 was inappropriate for Ariane-5.*
   BP #20: *Database confusion over reference trajectories.*
   BP #17: *Failure to adhere to "Test as You Fly" approach*.

2. **Switchover to the backup unit was accomplished, but SRI-2 immediately failed in the same way as SRI-1.**

   BP # 7: *Evaluate if redundancy using identical GN&C components increases or decreases reliability.*

3. **The OBC could not switch back to SRI-1 so it accepted SRI-2 diagnostic data as attitude data and generated improper TVC commands.**

   BP #3: *Ensure that Abort/Safe Haven strategies/functions are properly implemented. Ariane-5 was lacking a simple and reliable "Never Give Up" flight control capability.*

Recommendations & Summary

General Recommendations for Human-Rated Spacecraft GN&C DDT&E

- **Fully understand the specific GN&C architectural drivers arising from each mission operational phase**
  - Factor in the human response time constraints in the GN&C reliability trades for highly dynamic mission phases
  - Carefully consider and define requirements for autonomous fault detection and response capabilities during ascent, rendezvous, and EDL operations
- **Keep It Simple: Avoid introducing complexity in the GN&C subsystem**
- **Avoid an overly narrow GN&C discipline-specific approach**
  - Mishaps often occur because of an inability to consistently think at a system-level
- **Don't overly focus on the implementation of new GN&C capabilities to the point where previously flight-proven functions are impacted or lost**
- **Always ensure there is a simple and reliable "Never Give Up" GN&C backup mode capable of returning the crew safely to Earth**

Recommended Key Elements for GN&C DDT&E Process

- **Many GN&C DDT&E problems and issues can be avoided with a proactive multi-pronged approach that includes the following elements:**
  - Team wide emphasis on safety and mission success
  - Open and clear communication across entire Project team
  - Maintaining a systems-level perspective while working discipline-specific issues
  - Rigorous failure mode analysis (including degraded modes of operation)
  - Formulating a common understanding of what can go wrong during the mission
  - Contingency planning based on consequences of what can go wrong
  - Formal risk analysis and trades
  - Infusion of Lessons Learned
  - Consideration and attention to Best Practices
  - Holding independent non-advocate peer reviews
  - Exploiting external expert knowledge and technical support when needed

Summary

- **This presentation has introduced the initial set of the NESC GN&C DDT&E Best Practices for review and comment by the Program Management community**

- **The NESC GN&C Technical Discipline Team (TDT) intends to build upon and expand the work done to date in this area**
  - Objective is to define and broadly share a comprehensive set of Agency-wide GN&C subsystem DDT&E guidelines

- **We welcome and solicit constructive feedback from the Program Management community as we go forward with this activity**

- **Call Neil Dennehy at NASA/GSFC on 301-286-5696 (or e-mail at *cornelius.j.dennehy@nasa.gov*) with your:**
  - **Comments**
  - **Questions**
  - **Experiences**
  - **Inputs**

Backup

Top-Level Summary of the X-43A Mishap

The HXLV (Pegasus) was used to accelerate the Hyper-X Research Vehicle (HXRV) to the required Mach number and operational altitude for demonstration.

- **The trajectory that was selected to achieve the mission was at a lower altitude (i.e. a higher dynamic pressure) than a typical Pegasus trajectory.**
- **Flight went as planned after B-52 drop until pitch-up maneuver.**
- **Diverging roll oscillation at 2.5-Hz frequency occurred during pitch-up.**
- **Roll oscillation continued to diverge until about 13 seconds into flight.**
- **Rudder electro-mechanical actuator stalled & ceased to respond to autopilot at that point causing loss of yaw control.**
- **Loss of yaw control caused X-43A stack sideslip to diverge rapidly to over 8º.**
- **Structural overload of starboard elevon occurred at 13.5 seconds**
- **Loss of control caused X-43A stack to deviate significantly from planned trajectory.**
- **Vehicle terminated by range control about 49 seconds after release.**

Root Causes of the X-43A Mishap vs. NESC GN&C Best Practices

1. **The vehicle control system design was deficient for the trajectory flown due to inaccurate analytical models which overestimated design margins.**
   - **BP #8: *Over-reliance/Over-Confidence on Pegasus heritage*.**
   - **BP #17: *Failure to adhere to "Test as You Fly" approach.***
2. **Failure triggered by divergent roll oscillatory motion at 2.5 Hz, caused by excessive control system gain.**
   - **BP #12: *Insufficient control system stability margins.***
3. **Modeling inaccuracies in fin actuation system & aerodynamics. Insufficient variations of modeling parameters.**
   - **BP #13: *Lacking parametric uncertainty analysis for control system.***
4. **Rudder actuator stall occurred as consequence of divergent roll which accelerated loss of control.**
   - **BP #14: *Inadequate dynamic modeling.***
5. **Flight failure was only reproduced when all modeling inaccuracies with uncertainty variations were incorporated in system-level linear analysis model & nonlinear simulation model.**
   - **BP #15: *Independent Truth Model should have identified un-modeled effects.***

Top-Level Summary of the TIMED Mishap

The Thermosphere, Ionosphere, Mesosphere, Energetics and Dynamics (TIMED) spacecraft was launched on 7 December 2001 into low Earth orbit. There were 4 separate GN&C anomalies early in the mission:

1. Shortly after separation there was a steady increase in spacecraft system momentum.

2. Coming out of eclipse and seeing the Sun for the first time in Sun Pointing Mode, the spacecraft pointed an incorrect axis toward the Sun.

3. The Nadir Pointing Mode, which is used for Science observations, had an unanticipated 2.1 Hz oscillation.

4. Momentum dumping occurred 10 times/day rather than the expected once/day.

Root Causes of the TIMED Mishap vs. NESC GN&C Best Practices

1. **There was a Sign Error in the Momentum Unloading Control Logic.**
   BP #18: ***True end-to-end sensors-to-actuators polarity tests not conducted.***
2. **Two of the Sun Sensors were not in the flight configuration during ACS polarity test.**
   BP #17: ***"Test As You Fly" philosophy was not enforced.***
3. **There was a Controls-Structures Interaction (CSI) with the Solar Array Flex Mode which varied from 2.0-2.6 Hz depending on array orientation.**
   BP #2: ***Interactions between GN&C, Power, and Structures were not well defined.***
   BP #12: ***Stability margins were not robust to parameter variations.***
4. **The Spacecraft had a 10 A-m^2 Residual Magnetic Dipole.**
   BP #2: ***Residual dipole requirement was not specified.***
   BP #17: ***Residual dipole was not measured in ground test.***